Application No.: 09/872,077
Amendment Dated 08/29/2005
Reply to Office Action of 06/29/2005

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, comprising:
said data element being statically encrypted with said static key;
said data element being dynamically encrypted with said dynamic key; and
said data element being decrypted with said dynamic key and said static key on a receiving computer system, wherein in response to a transmission failure of said data element, decryption of said data element being recovered without retransmission of data.

2. (original) The computer system of Claim 1, wherein encryption with said static key is strong encryption.

3. (original) The computer system of Claim 1, wherein encryption with said dynamic key is weak encryption.

4. (currently amended) The computer system of Claim 1, wherein:
said data element is encrypted with said static key on a first computer system;
said data element is encrypted with said dynamic key on a second computer system;
~~said data element is decrypted with said static key and said dynamic key on a third computer system;~~ and
thereby encryption and decryption are distributed between said first computer system, said second computer system, and said receivingthird computer system.

5. (Original) The computer system of Claim 4, wherein said second computer system is untrusted.

6. (currently amended) The computer system of Claim 1, wherein:
said data element is encrypted with said static key on a first computer system;

said data element is encrypted with said dynamic key on said first computer system;

~~said data element is decrypted with said static key and said dynamic key on a second computer system;~~ and

thereby encryption and decryption are distributed between said first computer system and said receiving~~second~~ computer system.

7. (currently amended) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, comprising:
encrypting said data element with said static key;
encrypting said data element with said dynamic key; ~~and~~
transmitting said encrypted data element to a receiving computer system;
decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system; and
determining when transmission of said encrypted data element failed; and
recovering said decrypting of said encrypted data element without retransmission of data.

8. (currently amended) The method of Claim 7, ~~further comprising~~wherein said encrypting said data element with said static key strongly encrypts~~enerypting~~ said data element with said static key.

9. (currently amended) The method of Claim 7, ~~further comprising~~wherein said encrypting said data element with said dynamic key weakly encrypts~~enerypting~~ said data element with said dynamic key.

10. (currently amended) The method of Claim 7, further comprising:
wherein said encrypting said data element with said static key is on a first computer system;
transmitting said data element to a second computer system;
wherein said encrypting said data element with said dynamic key is on said second computer system;
~~transmitting said data element to a third computer system;~~

~~decrypting said data element with said static key and said dynamic key on said third computer system;~~ and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving ~~third~~ computer system.

11. (currently amended) The method of Claim 7, ~~further comprising:~~

wherein said encrypting said data element with said static key is on a first computer system;

wherein said encrypting said data element with said dynamic key is on said first computer system;

~~transmitting said data element to a second computer system;~~

~~decrypting said data element with said static key and said dynamic key on said second computer system;~~ and

thereby distributing encryption and decryption between said first computer system and said receiving~~second~~ computer system.

12. (currently amended) The method of Claim 10, further comprising:

determining when transmission of said data element from said first computer system to said second computer system failed; and

recovering said decrypting of ~~repairing~~ said data element without retransmission of said data.

13. (canceled)

14. (canceled)

15. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt a data element and decrypt said data element using a static key and a dynamic key, comprising:

encrypting said data element with said static key;

encrypting said data element with said dynamic key; ~~and~~

transmitting said encrypted data element to a receiving computer system;

decrypting said encrypted data element with said static key and said dynamic key on said receiving computer system;

determining when transmission of said encrypted data element failed; and

recovering said decrypting of said encrypted data element without retransmission of data.

16. (currently amended) The article of manufacture of Claim 15 ~~further comprising~~wherein said encrypting said data element with said static key strongly encrypts~~encrypting~~ said data element with said static key.

17. (currently amended) The article of manufacture of Claim 15 ~~further comprising~~wherein said encrypting said data element with said dynamic key weakly encrypts~~encrypting~~ said data element with said dynamic key.

18. (currently amended) The article of manufacture of Claim 15, further comprising:

wherein said encrypting said data element with said static key is on a first computer system;

transmitting said data element to a second computer system;

wherein said encrypting said data element with said dynamic key is on said second computer system;

~~transmitting said data element to a third computer system;~~

~~decrypting said data element with said static key and said dynamic key on said third computer system~~; and

thereby distributing encryption and decryption between said first computer system, said second computer system, and said receiving~~third~~ computer system.

19. (currently amended) The article of manufacture of Claim 15, ~~further comprising:~~

wherein said encrypting said data element with said static key is on a first computer system;

wherein said encrypting said data element with said dynamic key is on said first computer system;

~~transmitting said data element to a second computer system;~~

~~decrypting said data element with said static key and said dynamic key on said second computer system;~~ and

thereby distributing encryption and decryption between said first computer system and said receiving~~second~~ computer system.

20. (currently amended) The article of manufacture of Claim 18, further comprising:
determining when transmission of said data element from said first computer system to said second computer system failed; and
recovering said decrypting of~~repairing~~ said data element without retransmission of said data.

21. (canceled)

22. (canceled)

23. (currently amended) A computer system for encrypting and decrypting a data element using a static key and a dynamic key, said data element being partitioned into a plurality of chunks, comprising:
said data element chunks being statically encrypted with said static key;
said data element chunks being dynamically encrypted with said dynamic key; and
said data element chunks being decrypted with said dynamic key and said static key on a receiving computer system, wherein in response to a transmission failure of one of said data element chunks, decryption of said data element chunks being recovered without retransmission of data.

24. (original) The computer system of Claim 23 wherein encryption with said static key is strong encryption.

25. (original) The computer system of Claim 23, wherein encryption with said dynamic key is weak encryption.

26. (currently amended) The computer system of Claim 23, wherein:
said data element chunks are encrypted with said static key on a first computer system;
said data element chunks are encrypted with said dynamic key on a second computer system;

~~said data element chunks are decrypted with said static key and said dynamic key on a third computer system;~~ and

thereby encryption and decryption are distributed between said first computer system, said second computer system, and said receiving~~third~~ computer system.

27. (original) The computer system of Claim 26, wherein said second computer system is untrusted.

28. (currently amended) The computer system of Claim 23, wherein:

said data element chunks are encrypted with said static key on a first computer system;

said data element chunks are encrypted with said dynamic key on said first computer system;

~~said data element chunks are decrypted with said static key and said dynamic key on a second computer system;~~ and

thereby encryption and decryption are distributed between said first computer system and said receiving~~second~~ computer system.

29. (currently amended) A computer implemented method for encrypting a data element and decrypting said data element using a static key and a dynamic key, said data element being partitioned into chunks, comprising:

encrypting said data element chunks with said static key to provide static encrypted data element chunks;

encrypting said static encrypted data element chunks with said dynamic key to provide dynamic-static data element chunks and dynamic encryption recovery information states; ~~and~~

transmitting said dynamic-static data element chunks and said dynamic encryption recovery information states to a receiving computer system;

decrypting said dynamic-static data element chunks with said static key and said dynamic key on said receiving computer system;

determining, on said receiving computer system, when transmission of one of said dynamic-static data element chunks failed; and

recovering, on said receiving computer system, said decrypting of said dynamic-static data element chunks after said one of said dynamic-static data element chunks based on one of said dynamic encryption recovery information states.

30. (currently amended) The method of Claim 29 ~~further comprising~~wherein said encrypting said data element chunks with said static key strongly encrypts~~encrypting~~ said data element chunks with said static key.

31. (currently amended) The method of Claim 29 ~~further comprising~~wherein said encrypting said static encrypted data element chunks with said dynamic key weakly encrypts~~encrypting~~ said data element chunks with said dynamic key.

32. (currently amended) The method of Claim 29, further comprising:

wherein said encrypting said data element chunks with said static key is on a first computer system;

transmitting said static encrypted data element chunks to a second computer system;

wherein said encrypting said static encrypted data element chunks with said dynamic key is on said second computer system;

~~transmitting said data element chunks to a third computer system;~~

~~decrypting said data element chunks with said static key and said dynamic key on said third computer system; and~~

thereby distributing encryption between said first computer system and, said second computer system~~, and said third computer system~~.

33. (currently amended) The method of Claim 29, ~~further comprising:~~

wherein said encrypting said data element chunks with said static key is on a first computer system;

wherein said encrypting said static encrypted data element chunks with said dynamic key is on said first computer system;

~~transmitting said data element chunks to second computer system;~~

~~decrypting said data element chunks with said static key and said dynamic key on said second computer system; and~~

~~thereby distributing encryption between said first computer system and said second computer system~~.

34. (currently amended) The method of Claim 32, further comprising:

transmitting said static encrypted data element chunks with static encryption recovery information;

determining when transmission of said static encrypted data element chunks from said first computer system to said second computer system failed; and

recovering said decrypting of ~~repairing~~ at least one of said data element chunks without retransmission of said data based on said static encryption recovery information.

35. (canceled)

36. (canceled)

37. (currently amended) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer for causing a computer system to encrypt a data element and decrypt said data element using a static key and a dynamic key, said data element being partitioned into chunks, comprising:

encrypting said data element chunks with said static key;

encrypting said data element chunks with said dynamic key; ~~and~~

transmitting said data element chunks to a receiving computer system;

decrypting said data element chunks with said static key and said dynamic key on said receiving computer system;

determining when transmission of said data element chunks from said second computer system to said receiving computer system failed; and

recovering said decrypting of said data element chunks without retransmission of said data.

38. (currently amended) The article of manufacture of Claim 37 ~~further comprising~~wherein said encrypting said data element chunks said static key weakly encrypts~~encrypting~~ said data element chunks with said static key.

39. (currently amended) The article of manufacture of Claim 37 ~~further comprising~~wherein said encrypting said data element chunks with said dynamic key weakly encrypts~~encrypting~~ said data element chunks with said dynamic key.

40. (currently amended) The article of manufacture of Claim 37, further comprising:

wherein said encrypting said data element chunks with said static key is on a first computer system;

transmitting said data element chunks to a second computer system;

wherein said encrypting said data element chunks with said dynamic key is on said second computer system;

~~transmitting said data element chunks to a third computer system;~~

~~decrypting said data element chunks with said static key and said dynamic key on said third computer system;~~ and

thereby distributing encryption between said first computer system and~~,~~ said second computer system~~, and said third computer system~~.

41. (currently amended) The article of manufacture of Claim 37, ~~further comprising:~~

wherein said encrypting said data element chunks with said static key is on a first computer system;

wherein said encrypting said data element chunks with said dynamic key is on said first computer system~~;~~

~~transmitting said data element chunks to a second computer system;~~

~~decrypting said data element chunks with said static key and said dynamic key on said second computer system; and~~

~~thereby distributing encryption between said first computer system and said second computer system~~.

42. (currently amended) The article of manufacture of Claim 40, further comprising:

determining when transmission of said data element chunks from said first computer system to said second computer system failed; and

recovering said decrypting of ~~repairing~~ said data element chunks without retransmission of said data.

43. (canceled)

44. (canceled)